Proceedings of the 7th International Conference on Trends in Electronics and Informatics (ICOEI 2023)
IEEE Xplore Part Number: CFP23J32-ART; ISBN: 979-8-3503-9728-4

Face Detection based Secured ATM System with Two Step Verification using Fisher Face Method

Dr.V.Praveena , Associate Professor,
praveenav@drngpit.ac.in
Department of Computer Science and Engineering,
Dr.N.G.P. Institute of Technology,
Coimbatore

Aarthi S, Student,
aarthisivakumarr@gmail.com
Department of Computer Science and Engineering,
Dr.N.G.P. Institute of Technology,
Coimbatore

Anu Sankari S, Student,
19csanusankaris@drngpit.ac.in
Department of Computer Science and Engineering,
Dr.N.G.P. Institute of Technology,
Coimbatore

Girija K, Student,
19csgirijak@drngpit.ac.in
Department of Computer Science and Engineering,
Dr.N.G.P. Institute of Technology,
Coimbatore

Kirthivarsini M, Student,
19cskirthivarsinim@drngpit.ac.in
Department of Computer Science and Engineering,
Dr.N.G.P. Institute of Technology,
Coimbatore

2023 7th International Conference on Trends in Electronics and Informatics (ICOEI) | 979-8-3503-9728-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICOEI56765.2023.10125744

Abstract – **Automated teller machines (ATMs) are utilizedby almost everyone today. Due to the inconvenience of carrying an ATM card everywhere, people might forget to bring their card or PIN code. The ATM card could be broken, whichwould restrict the user from having access to theirmoney. An actual security solution is offered in this proposal. Technologies like Face recognition and Mobile app confirmation to increase the security ofaccounts and the privacy of users are included. When a user attempts to make a transaction after having their face recorded and stored in the bank's database, the system performs face detection using the ATM's camera and performs user face verification. If the invalid user needs to continue the transaction process, the OTP authentication should be made by the valid user in the Mobile application, so that the unauthorized person would continue the transaction.**

Keywords – ATM (Automated Teller Machine), Security, Face recognition, Mobile Application, OTP (One Time Password)

I.INTRODUCTION

Although there has been a good overall influence from the rapid advancement of science and technology, numerous financial institutions continue to be targets of theft and fraud. ATMs are always prepared to handle consumers' financial transactions and banking needs. The ATM's main advantage is that it eliminates the need to waste time driving to the bank and standing in line to dotransactions. ATMs have gained a lot of popularity amongthe general people as a result of their accessibility and overall user friendliness. Two distinct services are provided by the existing ATM system.

The first not only provides the consumer with the requested cash but also sends a message detailing the amount of money taken and the account balance. The latter is more advanced in that it allows credit card payments, accepts user deposits, and notifies the user of transactions andaccount information.

The pin-based verification is a requirement for the current ATM security authentication. Only those who are knowledgeable with their PIN (Personal Identification Number), which allows them to access their account, are permitted to usean ATM. A machine that is automated becomes vulnerable because of a security flaw. Manufacturers of ATMs continuously improve and addsecurity features so that customers can conduct banking operations without worry or difficulties.

The idea of an ATM security system based on face recognition has emerged in order to give users a genuine security solution. The project's

major goal is to lessen fraud caused by theft and fake ATM cards. The system will provide you the choice to process whatever transaction you want to make. Selecting "Facial recognition based transaction" is required by the user. The process will continue if it matches the database image; otherwise, it will be stopped. After selecting their branch name and providing the PIN that is required for the second step of verification if the image matches, the user can continue with the transaction. With the aid of a mobile application, a valid user can produce an OTP in order to prevent an unauthorized user from withdrawing funds. The invalid user can then use that OTP to continue the transaction.

II. LITERATURE SURVEY

Rashmi pote et al[1], customers must install the Smart Mobile Banking Application (SMBA) via the bank portal after registering their smartphones with the bank server. The customer should decide to use a password as authentication when beginning a cash withdrawal from SMBA. Cash withdrawals are committed to the bank's database after being started and after the bank server has successfully verified the password. The customer can transfer Personal Information by Quick Response (QR) Code and then visit the closest ATM to retrieve the cash.

Gokul S, Kukan S, Meenakshi K, Vishnu Priyan S S, Rohan Gini J. M.E.Harikumar [2] RFID and fingerprint authorization are the basis of the ATM's operation. After the user's recognised card number, authentication status, and access location have been verified by cross-referencing database data, the RFID number and details are received from them. The account holder is informed if the authorization is genuine or not when the information are verified. For security reasons, the person's face is also captured on camera by the device along with the date and time.

J. Patoliya, Miral M, Desai [3] , the Embedded Linux Platform serves as the foundation for the Smart ATM Security System idea. The image processing software OpenCV, which has expanded capabilities, is utilized to create the system on a Raspberry Pi board the size of a credit card. In order to provide security, a human face is first captured, and accuracy of the face detection is checked. The user is encouraged to modify their position in order to properly identify the face if it cannot be done Even so, if the face cannot be positively identified, a 3-digit OTP will be sent via SMS to the watchman's mobile number. When the watchman inputs the OTP using the keypad, the door to the ATM room will only unlock; otherwise, it will remain locked.

Soundari D V, Aravindh R, Edwin Raj K, Abishek S [4], This idea incorporates Face-id as a key into the current technique. The fact that each person's face ID is unique and cannot be used by anybody else than the user is an advantage. Machine learning and image processing technologies (such as the Eigenface algorithm) are employed for face-id scan implementation.

Apurva Taralekar, Gopalsingh Chouhan, Rutuja Tangade, Nikhilkumar Shardoor [5], Unauthorized access is prohibited via the biometric fingerprint authentication approach, which is one of the most secure systems available because fingerprints serve as a unique form of identification. Also, this technology guarantees a secure GSM-based transaction (OTP). When compared to the conventional ATM system, the proposed solution achieves superior security.

III. COMPARATIVE STUDY

[1] In the paper "Securing cash withdrawal from ATM with the help of Smart Mobile Banking Application" the three-factor authentication approach is proposed. For security purposes, the user can start a cash withdrawal from SMBA by entering a password. The consumer can visit a nearby ATM and receive the cash by scanning the QR code, which lengthens the transaction

procedure once the customer initiates the cash withdrawal and the bank server successfully authenticates the customer's password. Under our suggested approach, the transaction happens when the face is recognised and the OTP is entered, which speeds up the process.

[2] The paper "Face detection Open CV based ATM Security System" suggests biometric identification techniques as an alternative toPIN and ATM card usage. But, since ATM cards are not used in our idea, it is less complicated if oneof them is copied or misplaced.

[3] In light of the growing problem of fingerprint fraud, the article "Fingerprint sensorand RFID based ATM system using IOT" suggests a technique for carrying out transactions using RFID and fingerprint identification. We have implemented FaceID-based recognition in our system proposal,making fraud practically impossible.

[4] According to the paper "Biometric based Smart ATM using RFID," the transaction processcan only take place in places where access permission has been granted since it requires the verification of the ATM card number, authorization status, and access location beforeproceeding. Yet, the transaction procedure in our suggested solution can happen in any ATM machine in a trustworthy manner.

[5] The generation of OTP after the facial recognition phase can occasionally be delayed (i.e., If a particular network service is down, the user will be unable to get the OTP), which in turn makes user impatient. The paper "Enhanced Security for ATM Machine with OTP" also requires ATM card for transaction and the OTP is sent once to the designated mobile number after the face is recognized. So, to reduce the complexity of time in our system, we suggested a concept where the OTP is generatedbefore the user authorizes a family member or friend to withdraw money.

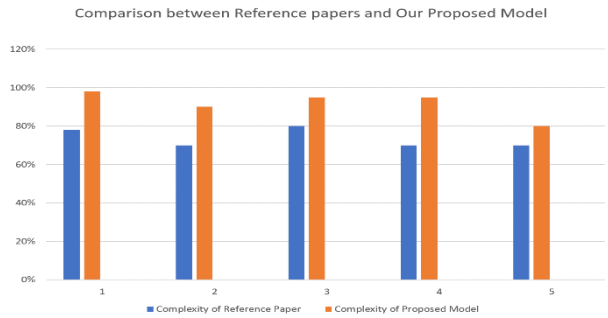

Figure 1 : Comparing the complexity of other papers and our proposed model

IV. SYSTEM ARCHITECTURE

A. EXISTING SYSTEM

The majority of users find it convenient andeasy to use the current ATMs. Existing ATMs typically display instructions on an ATM display screen that are read by a user in order to offer interactive operation of the ATM. A user can use and operate the ATM by entering data and information on a keypad after reading the instructions on the display. The pin-based verification method is a requirement of the current ATM security authentication method. Many factors, including urgency and unintended pin sharing, have an impact on the system. Magnetic chip cards are simple to duplicate.

Limitations of Existing System

1. Shoulder Surfing

Shoulder surfing is a technique for watching someone using a cash register or other electronic device in order to spy on them and learn their passwords and other personal information.

2. Spoofing

Impersonating someone else, gaining access to their account, and abusing it are all examples of spoofing.

3. Skimming

In order to obtain card information from a magnetic chip, thieves use card skimmer devices. Frequently, these gadgets are positioned within or on top of an ATM card reader.

4. Card Phishing

As the customer inserts their card into the ATMto make a purchase, a card phishing attempt isattempted to steal it. To capture the customer'scard, a gadget is positioned above or inside thecard slot. These devices are designed to prevent customers from getting their cards back following a transaction.

B. PROPOSED SYSTEM

The idea of an ATM security system based on facial detection has developed as a viable security solution for the public. To extract the textural features of the face for recognition, Haar- cascade and Fisher Face are used. Our project seeks to use an embedded ATM camera to detect faces using a computer vision framework. Face detection technology makes use of the user's face as a key to uniquely identify them. Automatic Teller Machines (ATMs) typically rely on pin-based verification for user authentication. To improve the security of consumer authentication at ATMs, numerous studies have been conducted.

In the first case, the customer must enroll their face in order to store it on the bank's server and register with the bank using their information. The datas are stored in the encrypted form in the cloud that makes the data safe from attacks.

When a consumer chooses to continue a transaction at an ATM using facial detection in the second scenario, the interfacecaptures the user’s face with the help of camera embedded in the Automated Teller Machine (ATM) and checks it with the database to verify whether the image matches or not. If the image matches the user needs to select their branch name and can proceed the transaction by enteringthe PIN which is given as the second step for verification.

In the third scenario, if the valid user wants the unauthorized user to withdraw his/her money, he/she can generate an OTP with the help of mobile application, therefore the invalid user can proceed the transaction with the help of that OTP as given in Figure :2.

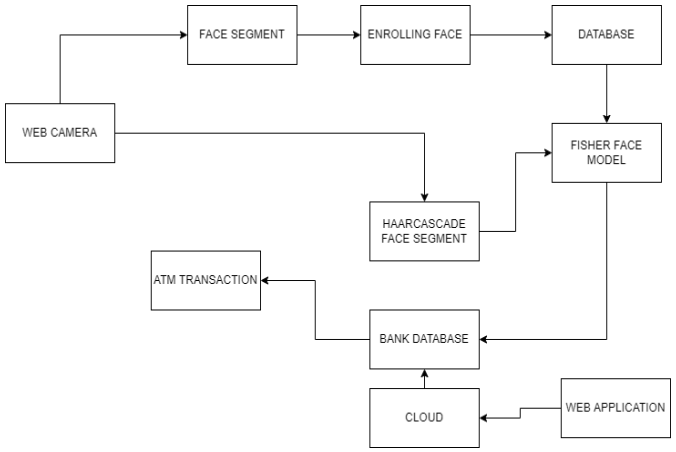

Figure 2 : Block diagram of proposed system

This accuracy of this model varies from face to face and the overall accuracy is 93.5 % and the predicting time of faces varies by system.

a) Fisher Faces Face Recognition Algorithm

The Eigenfaces method has been enhanced bythis one. Eigenfaces analyses all of the training faces from every person at once and identifies the principal components from each one taken individually. By doing so, it avoids concentrating on the characteristics that set one person apart from another.

Fisher Faces' face recognition system precisely extracts the key characteristics that set one person apart from the others. In that regard, one person's parts do not over shadow their counterparts. Fisherface uses the Principle Component

Analysis (PCA) and Linear Discriminant Analysis (LDA) methods to extract the characteristics of an image and detects the face based on the decrease in face space dimension. Fisherface is also resistant to the blurring and noise-induced picture effects. The accuracy with which various human expressions or emotions are recognised and calculated is measured using the FisherFace algorithm.

b) Haar Cascade Algorithm

Deep learning is used in the Haar Cascade method to identify faces. Face detection is made possible by employing a large number ofboth positive and negative photos to train a cascade function.

The first thing to do once the camera takesa picture is to extract the image's features. Let's say that we want to extract 160000+features from a single image with 8 × 8 pixels.The second stage is to train the algorithm with numerous positive and negative photos because face detection cannot beaccomplished using features from a single image. Features are extracted from eachimage using a threshold value, then all the features are combined and used for detection.The 160000+ features are then reduced to6000 features at this point.

When classifiers evaluate a small fraction of feature data with the acquired image, the next stage is face detection. The image is not detected as seen inFigure:3 if any of the features chosen do not match the obtained image.

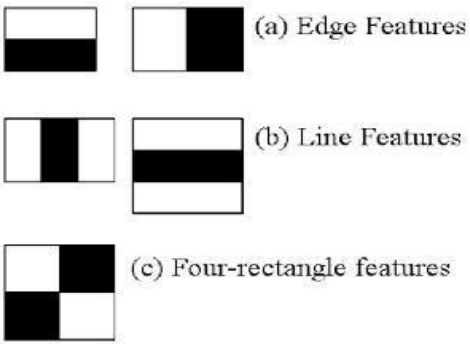

Figure 3 : Features of Haar Cascade Algorithm

V. RESULT

Case 1 : When face matched

The customer will be directed to the next step of the transaction, where they can select the branch name, if the face matches the image saved in the database.

Case 2 : When face doesn't match

If the face doesn't match the transaction will not be continued.

Case 3 : When the valid user wants the unauthorized user to perform transaction

If the authorised user needs to make a transaction, the authorised user can utilise themobile application to produce an OTP, which the unauthorised user can then use to complete the transaction.

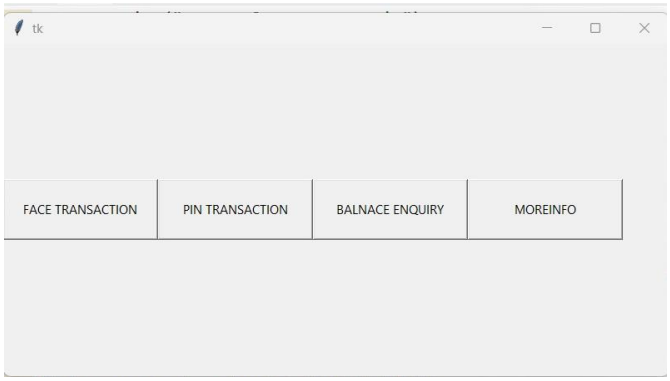

Figure 4 : Displaying options for proceeding transaction

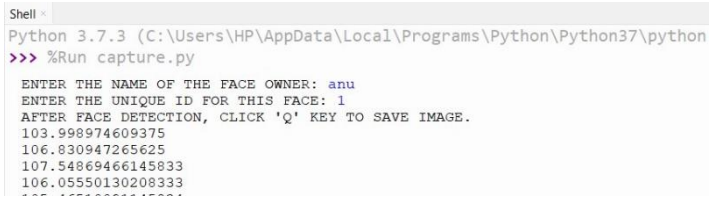

Figure 5 : Entering the details before capturing face.

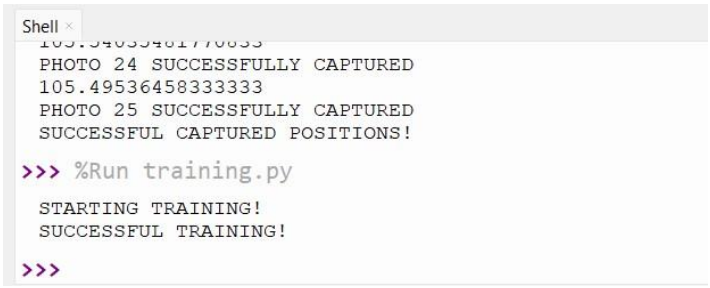

Figure 6 : After successfully training the datasets

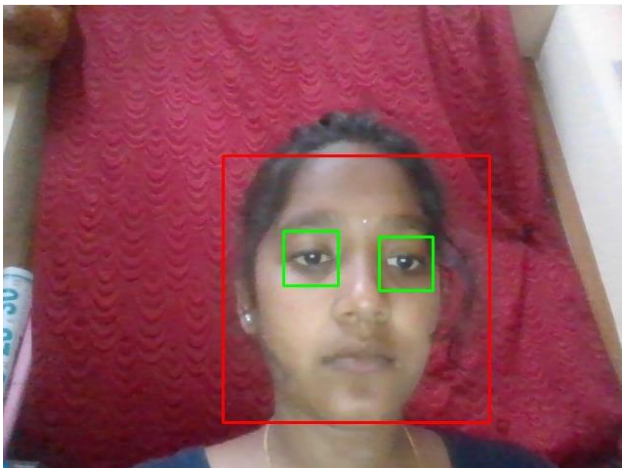

Figure 7 : Capturing face

Figure 8 : If the amount is successfully processed after selecting the bank

Figure 9 : GUI for setting OTP for unauthorized user's transaction

VI. CONCLUSION

Biometric Authentication for ATMs is a stronger method of authentication and verification as it is uniquely bound to individuals. An ATM design that uses facial recognition software coupled with OTP to provide more security. The proposed method helps in safe and secure transaction. The hackers can easily crack the PIN number by fixing the camera near ATM machine. The ATM card can also be duplicated. These can be avoided by the use of Face Recognition System. By using the PIN as second step of verification, the system achieves safer transaction. The unauthorized user can alsoperform transaction with the help of OTP generated in the application by the valid user. It is really useful because two level security system and a feature that the valid user can allow the invaliduser to perform transaction with the help of OTP generated in the application is added.

VII. REFERENCES

[1] J.J. Patoliya, M.M. Desai, Face Detection based ATM Security System using Embedded Linux Platform, 2nd International Conference for Convergence in Technology (I2CT), 2017.

[2] M. Karovaliyaa, S. Karediab, S. Ozac, Dr.D.R. Kalbande, Enhanced Security for ATM machine with OTP and Facial Recognition Features, International Conference on Advanced Computing Technologies and Applications (ICACTA), 2015.

[3] Sivakumar T, Gajjala Askok, Sai Venu, Design and Implementation of Security Based ATM theft Monitoring System, International Journal of Engineering Inventions, Volume 3, Issue 1, 2013.

[4] C.Bhosale, P.Dere, C.Jadhav, ATM security usingface and fingerprint recognition, International Journal of Research in Engineering, Technologyand Science, Volume VII, Special Issue, Feb 2017.

[5] Manoj V, M.Sankar R, Sasipriya S, U.Devi E, Devika T, Multi Authentication ATM Theft Prevention Using iBeacon , International Research Journal of Engineering and Technology (IRJET).

[6] L.Wang, H.Ji, Y.Shi, Face Recognition using Maximum Local Fisher Discriminant Analysis, 18th IEEE International Conference on Image Processing, 2011.

[7] K.Shailaja, Dr.B.Anuradha, Effective Face Recognition using Deep Learning based Linear Discriminant Classification, IEEE International Conference on Computational Intelligence and Computing Research, 2016.

[8] H.R.Babaei, O.Molalapata and A.H.Y.Akbar Pandor, Face Recognition Application for Automated Teller Machines (ATM), International Conference on Information and Knowledge Management (ICIKM), 2012.

[9] Rutuja Naval, Ankita Khot, Samruddhi Khedekar , Manjushree Sangale, Securing ATM Transaction OTP and Facial Recognition Features, International Journal of Advanced Research in Science, Communication Technology (IJARSCT), Volume 2, Issue 8, June 2022.

[10] DR S Sasipriya, Dr P Mayil Vel Kumar, S.Shenbagadevi, Face Recognition Based New Generation ATM System, European Journal of Molecular and Clinical Medicine, Volume 7, Issue 4, 2020.

[11] Bharti Thakur,Pof. Bhupinder Verma,"Design of an ATM Security Through Smart-Vision",2018 International Conference on Intelligent Circuits and Systems (ICICS)

[12] S Gokul,S Kukan,K Meenakshi,S S Vishnu Priyan,J Rolant Gini,M.E. Harikumar, Biometric Based Smart ATM Using RFID, Third International Conference on Smart Systems and Inventive Technology (ICSSIT), 2020.

[13] S. Shriram, Swastik B. Shetty, Vishnuprasad P. Hegde,K C R Nisha,V. Dharmambal, Smart ATM surveillance system, International Conference on Circuit Power and Computing Technologies (ICCPCT), 2016.

[14] Soundari D V,Aravindh R,Edwin Raj K,Abishek S, Enhanced Security Feature of ATMs Through Facial Recognition, 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021.

[15]Maddela Subha Sri,J.Krishna Chaithanya,Nelli Dhruthiee, Design and Implementation of Smart ATM under IDLE Application, 7th International Conference on Communication and Electronics Systems (ICCES), 2022